UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/966,890	09/28/2001	E. David Neufeld	COMP:0224	4334

7590 10/02/2008

Intellectual Property Administration
Legal Dept., M/S35
P.O. Box 272400
Ft. Collins, CO 80527-2400

EXAMINER	
TESLOVICH, TAMARA	
ART UNIT	PAPER NUMBER
2137	

MAIL DATE	DELIVERY MODE
10/02/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/966,890	NEUFELD ET AL.	
	Examiner	Art Unit	
	Tamara Teslovich	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on *16 July 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *13-18,27,29-32,35 and 41* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *13-18,27,29-32,35 and 41* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on July 16, 2008 has been entered.

Claims 1-12, 19-26, 28, 33-34, and 36-40 are cancelled.

Claims 13 and 27 are amended.

Claims 13-18, 27, 29-32, 35, and 41 are pending and herein considered.

Response to Arguments

Applicant's arguments filed July 16, 2008 have been fully considered but they are not persuasive.

Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention *without specifically pointing out how the language of the claims patentably distinguishes them* from the references.

In response to Applicant's first set of arguments, the recitation “a method of populating a portion of a seed pool with a signature value so as to allow a bypass of a

cryptographic security subsystem of a processor-based device for a period of time" has not been given patentable weight because the recitation occurs in the preamble. A preamble is generally not accorded any patentable weight where it merely recites the purpose of a process or the intended use of a structure, and where the body of the claim does not depend on the preamble for completeness but, instead, the process steps or structural limitations are able to stand alone. See *In re Hirao*, 535 F.2d 67, 190 USPQ 15 (CCPA 1976) and *Kropa v. Robie*, 187 F.2d 150, 152, 88 USPQ 478, 481 (CCPA 1951).

Furthermore, Applicant's use of the phrases "so as to allow," "thus allowing," "thus terminating," and "thus bypassing" have not been given weight because they simply express the intended result of the process step positively recited. The subject matter of a properly construed claim is defined by the terms that limit its scope. As a general matter, the grammar and intended meaning of terms used in a claim will dictate whether the language limits the claim scope. Language that suggests or makes optional but does not require steps to be performed or does not limit a claim to a particular structure does not limit the scope of a claim or claim limitation. The following are examples of language that may raise a question as to the limiting effect of the language in a claim:

(A) statements of intended use or field of use,

(B) "adapted to" or "adapted for" clauses,

(C) "wherein" clauses, or

(D) "whereby" clauses.

This list of examples is not intended to be exhaustive. See also MPEP § 2111.04. The determination of whether each of these clauses is a limitation in a claim depends on the specific facts of the case. In Hoffer v. Microsoft Corp., 405 F.3d 1326, 1329, 74 USPQ2d 1481, 1483 (Fed. Cir. 2005), the court held that when a "whereby' clause states a condition that is material to patentability, it cannot be ignored in order to change the substance of the invention." Id. However, the court noted (quoting Minton v. Nat 'l Ass 'n of Securities Dealers, Inc., 336 F.3d 1373, 1381, 67 USPQ2d 1614, 1620 (Fed. Cir. 2003)) that a "whereby clause in a method claim is not given weight when it simply expresses the intended result of a process step positively recited.'" Id. Claims are to be given their broadest reasonable interpretation in light of supporting disclosure. In re Morris, 127 F.3d 1048, 1054-55, 44 USPQ2d 1023, 1027-28 (Fed. Cir. 1997). Limitations appearing in the specification but not recited in the claim should not be read into the claim. E-Pass Techs., Inc. v. 3Com Corp., 343 F.3d 1364, 1369, 67 USPQ2d 1947, 1950 (Fed. Cir. 2003) (claims must be interpreted "in view of the specification" without importing limitations from the specification into the claims unnecessarily). In re Prater, 415 F.2d 1393, 1404-05, 162 USPQ 541, 550-551 (CCPA 1969). See also In re Zletz, 893 F.2d 319, 321-22, 13 USPQ2d 1320, 1322 (Fed. Cir. 1989) ("During patent examination the pending claims must be interpreted as broadly as their terms reasonably allow.... The reason is simply that during patent prosecution when claims can be amended, ambiguities should be recognized, scope and breadth of language explored, and clarification imposed.... An essential purpose of patent examination is to fashion claims that are precise, clear, correct, and unambiguous. Only in this way can

uncertainties of claim scope be removed, as much as possible, during the administrative process.").

In response to Applicant's next set of arguments regarding the Examiner's alleged "suggest[ion] that the primary and sole purpose of the Applicant's signature value is to increase entropy and make it more difficult for unauthorized access to the system," the Examiner respectfully reminds Applicant that a recitation of the intended use of the claimed invention must result in a structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art. If the prior art structure is capable of performing the intended use, then it meets the claim.

In response to Applicant's next set of arguments regarding Applicant's "primary focus [being] placed on bypassing the cryptographic security subsystem for a period of time to allow access to the processor-based device" the Examiner reminds Applicant that a recitation of the intended use of the claimed invention must result in a structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art and that material in the preamble is generally not accorded any patentable weight where it merely recites the purpose of a process or the intended use of a structure, and where the body of the claim does not depend on the preamble for completeness but, instead, the process steps or structural limitations are able to stand alone. Were it Applicant's intention to claim the bypass of a cryptographic subsystem he may do so through the positive recitation of limitations directed to those ends. Insofar as Applicant's claims fail to positively recite such

limitations, it is noted that the features upon which applicant relies (i.e., “bypassing the cryptographic security subsystem for a period of time to allow access to the processor-based device”) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

In response to Applicant's argument that the references fail to show certain features of applicant’s invention, it is noted that the features upon which applicant relies (i.e., “the counter variable and constant are being processed, tracked, and evaluated") are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

In response to Applicant's next set of argument that the references fail to show certain features of applicant’s invention, it is noted that the features upon which applicant relies (i.e., “the Applicant’s signature value, within the input seed, can change based on a masking of the least significant bit of a timer into the input seed at a location in memory indicated by an incremented pointer") are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

It is based upon the argument above in view of the references in their entirety that the Examiner maintains her 35 USC 102(e) rejections of pending claims 13-18, 27, 29-32, 35, and 41, included below in a form to reflect Applicant's amendments.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 13-18, 27, 29-32, 35, and 41 are rejected under 35 U.S.C. 102(e) as being anticipated by US Patent Application Publication No. 2002/0172359 A1 to Markku-Juhani Saarinen, hereinafter referred to as *Saarinen*.

Regarding **claim 13**, Saarinen discloses a method of populating a portion of a seed pool with a signature value so as to allow a bypass of a cryptographic security subsystem of a processor-based device for a period of time, the method comprising the acts of

(a) prior to enabling the cryptographic security subsystem, writing a plurality of bits of data to a seed pool, the plurality of bits of data having a signature value thus allowing the bypass of a cryptographic security subsystem (par 32);

(b) detecting occurrences of a first type of triggering event (par 32);

(c) writing one or more bits of data to the seed pool upon termination of the first type of triggering event, the one or more bits of data altering the signature value of the seed pool (par 32); and

(d) enabling the cryptographic security subsystem when more than a predetermined portion of the signature value of the seed pool has been altered thus terminating the bypass of the cryptographic security subsystem (pars 33, 72); and

(e) generating a pseudo-random number from the seed pool, wherein the pseudo-random number is used to generate the cryptographic key for the cryptographic security subsystem of the processor-based device (par 27).

Regarding **claims 14 and 15**, Saarinen discloses wherein the first type of triggering event comprises either a cycle of power applied to the processor-based device or a reboot of the processor-based device (pars 25, 27, 32, 33, 74).

Regarding **claim 16**, Saarinen discloses wherein act (c) comprises the act of masking the one or more bits of data into the seed pool (pars 27, 32, 33, 37, 42).

Regarding **claim 17**, Saarinen discloses wherein act (c) comprises the act of capturing the one or more bits of data from a free-running timer (pars 25, 27, 31, 32, 33).

Regarding **claim 18**, Saarinen discloses detecting a second type of triggering event; determining if the seed pool is full; and writing one or more bits of data to the seed pool upon termination of the second type of triggering event if the seed pool is not full (pars 33, 72).

Regarding **claim 27**, Saarinen discloses a processor-based device comprising:

a host processing system, the host processing system comprising a processor (pars 25, 34);

a communications management system in communication with the host processing system (pars 25, 34);

a memory system in communication with the host processing system and the communications management system (par 25),

wherein the communications management system comprises:

an interface controller (pars 25, 26, 32);

a non-volatile memory device to store a seed pool comprising a plurality of data bits (par 25, 28); and

security logic in communication with the interface controller and the non-volatile memory device, the security logic configured to establish a secure communication session between the processor-based device and an external device in communication with the processor-based device via the interface controller (pars 25-26), and wherein the security logic is configured to:

write one or more bits to the seed pool, wherein the one or more bits originate from a source external to the seed pool and alter a signature value (par 32);

determine whether the plurality of data bits in the seed pool has at least a portion of a signature value (par 33) and

disable establishment of the secure communication session if the plurality of data bits has at least a portion of the signature value, thus bypassing the cryptographic security subsystem and allowing access to the processor-based device for a period of time (par 33).

Regarding **claim 29**, Saarinen discloses a main power supply to supply power to the processor-based device, and wherein the first type of triggering event comprises a cycle of the power supplied by the main power supply (pars 74-75).

Regarding **claims 30-31**, Saarinen discloses wherein the security logic is configured to detect a second type of triggering event; determine whether the seed pool is fully populated; and write one or more data bits to the seed pool upon termination of the second type of triggering event if the seed pool is not fully populated (pars 33, 72) and wherein the second type of triggering event comprises receipt of a communication from the external device via the interface controller (pars 25, 27, 32).

Regarding **claim 32**, Saarinen discloses wherein the interface controller comprises a network interface controller (pars 25, 27, 32).

Regarding **claim 35**, Saarinen discloses wherein the security logic is configured to detect a first type of triggering event, and to write one or more data bits to the seed pool upon termination of the first type of triggering event (pars 25, 27, 32).

Regarding **claim 41**, Saarinen discloses a method of manufacturing a processor-based device comprising: providing a memory comprising a seed pool, wherein the seed pool contains a plurality of bits having a signature value (par 33); writing one or

more bits of data to the seed pool upon termination of a first type of triggering event (pars 25, 27, 32); and enabling a cryptographic security subsystem when more than a threshold amount of the signature value of the seed pool has been altered (par 33).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tamara Teslovich whose telephone number is (571) 272-4241. The examiner can normally be reached on Mon-Fri 8-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Tamara Teslovich/

Examiner, Art Unit 2137

/Emmanuel L. Moise/

Supervisory Patent Examiner, Art Unit 2137